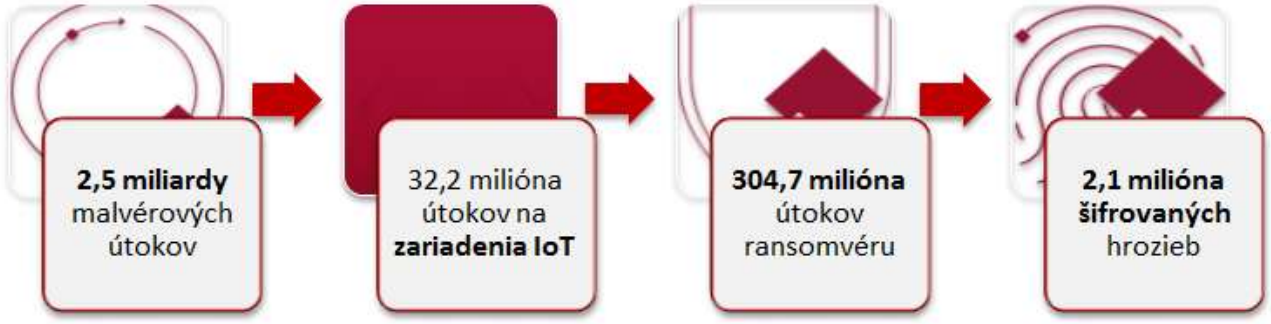
ALISON

Rast kybernetického zločinu v prvom polroku ohromil. Pozrite si čísla a typy útokov

Bojiská a konflikty sa presúvajú do kybernetického priestoru. Ransomvér vystrelil, malvér padol, útoky na IoT rastú a aj tie dobré správy sa ukazujú ako zle pochopené zlé správy. A Európa zbiera sily na spoločnú odolnosť.

Za prvý polrok 2021 svet počíta



Vydieračský softvér ide ako tornádo

Výskumný tím SonicWall Capture Labs zaznamenal v prvom polroku 304,7 milióna ransomvérových útokov, v júni dokonca rekordných 78,4 milióna pokusov za mesiac. Výročná správa založená na monitoringu sietí a zariadení varuje, že problém s ransomvérom sa naďalej zhoršuje, a medziročný rast o viac ako 150 percent to potvrdzuje.

Najčastejším cieľom útokov za šesť mesiacov roku 2021 sú vlády a štátne inštitúcie, ktoré zaznamenali trikrát viac útokov ako minulý rok. Vládne ciele čelia každý mesiac omnoho väčšiemu počtu útokov ako takmer všetky ostatné odvetvia. Alarmujúce nárasty počtov útokov zaznamenalo aj školstvo s nárastom o 615 percent a zdravotnícke organizácie s nárastom o 594 percent.

Viac ako polovica všetkých pokusov o ransomvérové útoky (64 %) sa pripisuje skupinám Ryuk, Cerber a SamSam. Ryuk produkciu v porovnaní s minulým rokom až strojnásobil.

Zariadenia IoT sú chutnučký cieľ

Počet zariadení pripojených do internetu sa dnes odhaduje na 13,8 miliardy. V prvej polovici roku 2021 zaznamenali výskumníci 32,2 milióna pokusov o malvérový útok na IoT zariadenia, čo je medziročný nárast o 59 percent.

Podľa špecializovaného portálu IoT Analytics sa má počet pripojených zariadení zvýšiť takmer až na 31 miliárd v roku 2025, čo znamená priemerne štyri IoT kúsky na obyvateľa planéty. Vzhľadom na tieto fascinujúce čísla bezpečnostné štandardy zostávajú podľa odborníkov až „šokujúco laxné“.

A mimochodom – ak by ste pozreli aj iné zdroje o počte zariadení, štúdie IDC predpovedajú až 55,7 miliardy IoT zariadení v roku 2025.

Jedna lepšia správa medzi zlými

Malvér dosiahol v roku 2020 šesťročné minimum, ale aj tak je počet 5,6 miliardy pokusov o útok ohurujúci. V prvom polroku 2021 bolo zaznamenaných 2,5 miliardy pokusov o útok, čo je pokles o 22 percent. Celkový objem ovplyvňuje pokles malvéru šíreného naslepo, no kompenzujú to sofistikované útoky.

„Menej škodlivého softvéru nie je to isté ako menej počítačovej kriminality," opäť trefne komentuje správa. Upúšťa sa od tradičných útokov v štýle gangstrov minulého storočia „spray-and-pray" v prospech špecializovaných, sofistikovaných a adresných útokov, schopných oveľa viac zarobiť a zanechať oveľa väčšiu škodu.

Nižší počet útokov dopĺňa ďalšie varovanie výskumníkov, že v roku 2021 pribudol počet malvérových hrozieb v kategórii „never-before-seen".

A Európa na čo čaká?

Európu potrápil v prvom polroku **234-percentný nárast** objemu ransomvéru, zatiaľ čo v Severnej Amerike narástol o 180 percent. V európskych krajinách malvér stúpal prudko najmä v Nemecku, ktoré zaznamenalo 150,4 milióna pokusov o útok, čo predstavuje medziročný nárast o 465 percent.

Škandál v podobe sledovacieho softvéru Pegasus určeného pre bezpečnostné služby na sledovanie zločincov bude rezonovať ešte veľmi dlho. Jediným členským štátom EÚ, ktorého vláda bola obvinená z použitia vojenskej technológie na tieto účely, bolo Maďarsko. Hackované a monitorované sú mobilné telefóny politikov, novinárov aj aktivistov, takže v nadväznosti na to Európska komisia potvrdila, že sa touto záležitosťou bude zaoberať.

Krížom cez hranice, segmenty a komunity

Európska komisia preto urýchľuje vytvorenie kybernetickej jednotky Joint Cyber Unit. Jej úlohou bude riešiť rastúci počet závažných kybernetických bezpečnostných incidentov ovplyvňujúcich verejné služby, podniky aj občanov Únie. Komisia vidí problém najmä v tom, že civilná oblasť, bezpečnostné agentúry, silové zložky, legislatíva, diplomacia, kybernetická obrana aj súkromný sektor často konajú bez spoločnej koordinácie a synergie.

Spoločná kybernetická jednotka má byť platformou na zabezpečenie koordinovanej reakcie EÚ na incidenty a krízy, ako aj na poskytovanie pomoci pri zotavovaní sa z kybernetických útokov. Cieľom je, aby jednotka prešla do operačnej fázy najneskôr do 30. júna 2022 a jej úplné zriadenie je plánované o rok neskôr.

ALISON

SonicWall Cyber Threat Report

State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time

IoT Growth Demands Rethink of Long-Term Storage Strategies, says IDC

Digital Brief powered by Facebook: Pegasus affair, Schrems III, online anonymity questioned

Kybernetická bezpečnosť v EÚ: Komisia navrhuje spoločnú kybernetickú jednotku na zintenzívnenie reakcie na rozsiahle kybernetickobezpečnostné incidenty